PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

Claims 1-11 (Canceled)

12. (Currently Amended) A method for generation of a cryptographic key by a wireless communication device, comprising:

generating a first public key for encrypting a first wireless communication;

generating, after termination of the first wireless communication and prior to initiation of a second secure wireless communication of the wireless communication device with a desired communication device, a second public key for transmission to the desired communication device, wherein the second public key is independent of the first public key;

storing the second public key in a memory of the wireless communication device prior to initiation of the second secure wireless communication with the desired communication device;

initiating, in response to ~~the~~ a user input, the second secure wireless communication of the wireless communication device with the desired communication device; and

transmitting the second public key to the desired communication device if the second public key is available in the memory.

13. (Canceled)

14. (Canceled)

15. (Previously Presented) The method of claim 32, further comprising:

generating a third public key to transmit to the desired communication device when it is determined that the second public key has not been stored.

16. (Currently Amended) A wireless communication device for generation of a cryptographic key, comprising:

means for generating a first public key for encrypting a first wireless communication;

means for generating, after termination of the first wireless communication and prior to initiation of a second secure wireless communication with a desired communication device, a second public key for transmission to the desired communication device, wherein the second public key is independent of the first public key;

means for storing the second public key in memory prior to initiation of the second secure wireless communication with the desired communication device;

means for initiating, in response to ~~the~~ a user input, the second secure wireless communication with the desired communication device; and

means for transmitting the second public key to the desired communication device if the second public key is available in the memory.

17. (Canceled)

18. (Canceled)

19. (Previously Presented) The wireless communication device of claim 33, further comprising:

means for generating a third public key to transmit to the desired communication device when it is determined that the second public key has not been stored.

20. (Currently Amended) A wireless communication device for generation of a cryptographic key, comprising:

a processor for:

generating a first public key to encrypt a first wireless communication;

generating, after termination of the first wireless communication and prior to initiation of a second secure wireless communication with a desired communication device, a second public key for transmission to the desired communication device;

storing the second public key in memory prior to initiation of the second secure wireless communication with the desired communication device

initiating, in response to ~~the~~ a user input, the second secure wireless communication with the desired communication device; and

transmitting the second public key to the desired communication device if the second public key is available in the memory;

the memory for storing the second public key,

wherein the second public key is independent of the first public key.

21. (Currently Amended) A processor for generation of a cryptographic key, said processor being configured to:

generate a first public key for encrypting a first wireless communication;

generate, after termination of the first wireless communication and prior to initiation of a second secure wireless communication with a desired communication device, a second public key for transmission to the desired communication device, wherein the second public key is independent of the first public key;

store the second public key in memory prior to initiation of the second secure wireless communication with the desired communication device;

initiate, in response to ~~the~~ a user input, the second secure wireless communication with the desired communication device; and

transmit the second public key to the desired communication device if the second public key is available in the memory.

22. (Currently Amended) A memory comprising instructions for generation of a cryptographic key, wherein the instructions upon execution cause a computer to:

generate a first public key for encrypting a first wireless communication;

generate, after termination of the first wireless communication and prior to initiation of a second secure wireless communication with a desired communication device, a second public key for transmission to the desired communication device, wherein the second public key is independent of the first public key;

store the second public key in memory prior to initiation of the second secure wireless communication with the desired communication device;

initiate, in response to ~~the~~ a user input, the second secure wireless communication with the desired communication device; and

transmit the second public key to the desired communication device if the second public key is available in the memory.

23. (Previously Presented) The memory of claim 22, wherein the instructions upon execution further cause a computer to:

determine whether the second public key has been stored prior to establishing the second wireless communication.

24. (Canceled).

25. (Previously Presented) The memory of claim 23, wherein the instructions upon execution further cause a computer to:

generate a third public key to transmit to the desired communication device when it is determined that the second public key has not been stored.

26. (Previously Presented) The processor of claim 21, wherein said processor is further configured to:

determine whether the second public key has been stored prior to establishing the second wireless communication.

27. (Canceled)

28. (Previously Presented) The processor of claim 26, wherein said processor is further configured to:

generate a third public key to transmit to the desired communication device when it is determined that the second public key has not been stored.

29. (Previously Presented) The wireless communication device of claim 20, wherein the processor determines whether the second public key has been stored prior to establishing the second wireless communication.

30. (Canceled)

31. (Previously Presented) The wireless communication device of claim 29, wherein the processor generates a third public key to transmit to the desired communication device when it is determined that the second public key has not been stored.

32. (Previously Presented) The method of claim 12, further comprising:

determining whether the second public key has been stored prior to establishing the second wireless communication.

33. (Previously Presented) The wireless communication device of claim 16, further comprising:

means for determining whether the second public key has been stored prior to establishing the second wireless communication.

34 - 43. (Canceled)